Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-6. (Canceled)

7. (Currently amended) [[The]] A method of ~~claim 5, further~~ authenticating a data processing device, comprising:

receiving an electrical signal having a data signal added therein, wherein the electrical signal is indicative of a location of the data processing device;

extracting the data signal from the electrical signal;

comparing data of the data signal to security information stored in the data processing device; and

permitting operation of the data processing device based on the comparison of the data of the data signal to the security information, wherein the method further comprises:

receiving a data packet from a sending device via a data network, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

comparing the second data value to the first data value;

permitting processing of the data packet if the second data value matches the first data value;

adding an identifier of the sending device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices; and

periodically clearing the list of authorized devices and the list of unauthorized devices.

8-17. (Canceled)

18. (Currently amended) [[The]] A computer program product in a recordable-type computer readable medium for authenticating a data processing device, ~~of claim 16, further~~ comprising:

first instructions for receiving an electrical signal having a data signal added therein, wherein the electrical signal is indicative of a location of the data processing device;

second instructions for extracting the data signal from the electrical signal;

third instructions for comparing data of the data signal to security information stored in the data processing device; and

fourth instructions for permitting operation of the data processing device based on the comparison of the data of the data signal to the security information, wherein the computer program product further comprises:

fifth instructions for receiving a data packet from a sending device via a data network, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

sixth instructions for querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

seventh instructions for comparing the second data value to the first data value;

eighth instructions for permitting processing of the data packet if the second data value matches the first data value;

ninth instructions for adding an identifier of the sending device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices; and

tenth instructions for periodically clearing the list of authorized devices and the list of unauthorized devices.

19-30. (Canceled)

31. (Currently amended) [[The]] A method of securing a data network, ~~claim 29, further~~ comprising:

receiving an electrical signal from an external electrical network;

adding a data signal to the electrical signal to generate a modified electrical signal, wherein the data signal includes security data, and wherein the modified electrical signal is indicative of a location of devices coupled to the data network;

outputting the modified electrical signal to a local electrical network; and

permitting operation of the devices on the data network based on an authentication of the devices using the data signal extracted from the modified electrical signal, wherein the method further comprises:

receiving a data packet from a second device, via a data network, in a first device, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

comparing the second data value to the first data value;

permitting processing of the data packet if the second data value matches the first data value;

adding an identifier of the second device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices; and

periodically clearing the list of authorized devices and the list of unauthorized devices.

32-39. (Canceled)